Listing of the Claims:

The following is a complete listing of all the claims in the application, with an indication of the status of each:

1. (Currently amended) A method for controlling access to digital information, comprising:

storing digital information in an encrypted form on a host system; ~~and~~

reproducing the digital information using a media player application on the host system, said reproducing step including degrading a reproduction quality of the digital information based on at least one of a time condition and a use condition;

storing data on the host system which correlates a first type of decryption key with a first type of reproduction quality degradation performed based on at least one of said time condition and said use condition;

storing said first type of decryption key on the host system; and

comparing said first type of decryption key to the data stored on the host system to identify said first type of reproduction quality degradation,

wherein said reproducing step includes degrading the reproduction quality of the digital information in accordance with the first type of reproduction quality degradation identified in said comparing step.

2. Canceled

3. (Currently amended) The method of claim 1 ~~2~~, further comprising:

storing additional data on the host system which correlates a second type of decryption key with information which indicates that the digital information is to be reproduced without degradation in quality;

storing said second type of decryption key on the host system; and

comparing said second type of decryption key to the additional data stored on the host system,

wherein said reproducing step includes reproducing the digital

information on said media player application without degradation in quality based on said additional data comparing step.

4. (Original)   The method of claim 3, wherein said information which indicates that the digital information is to be reproduced without degradation in quality instructs said media player application to permanently prevent the first type of reproduction quality degradation indicated by said first type of decryption key.

5. (Original) The method of claim 1, wherein said reproducing step includes degrading the reproduction quality of the digital information by altering a decompression of the digital information.

6. (Original) The method of claim 1, wherein said reproducing step includes degrading the reproduction quality of the digital information by altering a rendering of the digital information.

7. (Original) The method of claim 1, wherein the host system is one of a personal computer, a personal digital assistant, and a digital set-top box.

8. (Original) The method of claim 1, wherein the media player application includes tamper-resistant software.

9. (Original) A method for controlling access to digital information, comprising:
     acquiring digital information for reproduction on a host system;
     sending the digital information to the host system with a first decryption key, said first decryption key instructing an application program on the host system to degrade the reproduction quality of the digital information based on at least one of a time condition and a use condition.

10. (Original) The method of claim 9, further comprising:
     receiving information from a user of the host system, said information

indicating a desire to have unrestricted access to the digital information; and

sending a second decryption key to the host system, said second decryption key instructing the application program to reproduce the digital information without degradation in quality.

11. (Original) The method of claim 10, wherein said second decryption key instructs the application program to reproduce the digital information without degradation.

12. (Original) The method of claim 9, wherein said first decryption key instructs the application program to degrade the reproduction quality of the digital information by altering a decompression of the digital information.

13. (Original) The method of claim 9, wherein said first decryption key instructs the application program to degrade the reproduction quality of the digital information by altering a rendering of the digital information.

14. (Original) The method of claim 9, wherein said sending step includes:

sending the application program with the digital information and said first decryption key.

15. (Original) The method of claim 14, wherein the application program performs a tamper-resistance function when executed on the host system.

16. (Original) The method of claim 14, further comprising:

storing data in the application program which correlates said first decryption key with a first type of reproduction quality degradation performed based on at least one of said time condition and said use condition, wherein the application program performs the first type of reproduction quality degradation when executed on the host system.

17. (Original) The method of claim 16, further comprising:

storing additional data in the application program which correlates a second decryption key with information indicating that the digital information is to be reproduced by the application without degradation in quality; and

sending said second decryption key to the host system,

wherein said application program compares said second decryption key to said additional data and then reproduces the digital information without degradation in quality.

18. (Original) The method of claim 17, wherein said second decryption key instructs the application program to permanently prevent the reproduction quality degradation of the digital information performed by said first decryption key.

19. (Original) The method of claim 16, further comprising:

storing additional data in the application program which correlates a second decryption key with a second type of reproduction quality degradation, said second type of reproduction quality degradation being less severe than the first type of reproduction quality degradation;

sending said second decryption key to the host system,

wherein said application program compares said second decryption key to said additional data and then reproduces the digital information with said second type of reproduction quality degradation.

20. (Original) The method of claim 11, further comprising:

defining a pricing structure wherein said second decryption key is priced higher than said first decryption key.

21. (Currently amended) A method for controlling access of digital information, comprising:

storing digital information in an encrypted form on a host system;

reproducing said digital information, using a first decryption key, a first

time with a first quality of reproduction, and

reproducing said digital information a second time, using a second

decryption key, with a second quality of reproduction, said second quality of

reproduction being degraded relative to said first quality of reproduction.

22. Canceled

23. (Original) A method for controlling access of digital information, comprising:

storing digital information in an encrypted form on a host system;

storing an application program for reproducing the digital information on

the host system;

storing a first decryption key on the host system; and

activating the application program to reproduce the digital information on

the host system, said application program reproducing the digital information

based on said first decryption key, said first decryption key controlling said

application program to reproduce only a portion of the digital information.

24. (Original) The method of claim 23, further comprising:

storing a second decryption key on the host system,

wherein said application program reproduces the digital information a

second time based said second decryption key, said second decryption key

controlling said application program to reproduce all of the digital information.